Comparison of Elliptic Curve and Edwards Curve

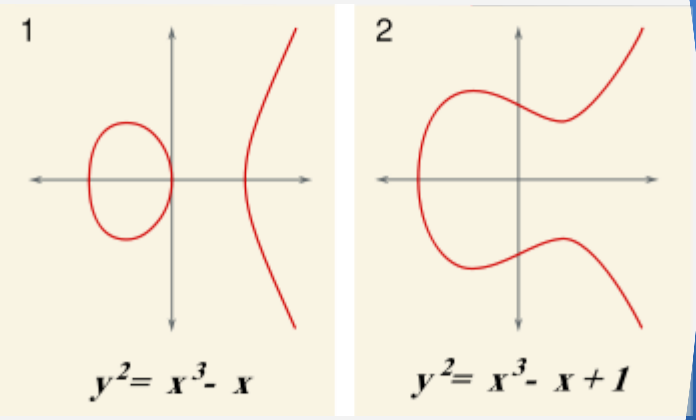
Shivapriya Hiremath
Stephanie Smith

Overview

- Elliptic Curve
  - Point Addition
  - Point Doubling
  - Point Multiplication
- Edwards Curve
  - Point Addition
- Results
- Random Number Generator using Edwards Curve

Elliptic Curve

- a smooth, projective algebraic curve of genus one
- can be written as a plane algebraic curve defined by an equation of the form $y^2 = x^3 + ax + b$
- non-singular (no cusps, self intersections, or isolated points)



Point Addition

- taking two points along a curve E and computing where a line through them intersects the curve
  - use the negative of the intersection point
- $(x_p, y_p) + (x_q, y_q) = (x_r, y_r)$

$$\lambda = \frac{3x_p^2 + 2ax_p + b}{2y_p}$$

$$x_r = \lambda^2 - a - 2x_p$$

$$y_r = \lambda(x_p - x_r) - y_p$$

Projective Point Addition

$$\begin{aligned}
\lambda_1 &= X_1 Z_2^2 \\
\lambda_2 &= X_2 Z_1^2 \\
\lambda_3 &= \lambda_1 - \lambda_2 \\
\lambda_4 &= Y_1 Z_2^3 \\
\lambda_5 &= Y_2 Z_1^3 \\
\lambda_6 &= \lambda_4 - \lambda_5 \\
\lambda_7 &= \lambda_1 + \lambda_2 \\
\lambda_8 &= \lambda_4 + \lambda_5 \\
Z_3 &= Z_1 Z_2 \lambda_3 \\
X_3 &= \lambda_6^2 - \lambda_7 \lambda_3^2 \\
\lambda_9 &= \lambda_7 \lambda_3^2 - 2X_3 \\
Y_3 &= (\lambda_9 \lambda_6 - \lambda_8 \lambda_3^3)/2
\end{aligned}$$

http://cs.ucsb.edu/~koc/ac/docs/w03/ecc-protocols.pdf

Point Doubling

- take the tangent of a single point and find the intersection with the tangent line

$$\lambda = \frac{3x_p^2 + 2ax_p + b}{2y_p}$$

$$x_r = \lambda^2 - a - 2x_p$$

$$y_r = \lambda(x_p - x_r) - y_p$$

Projective Doubling

$$
\begin{aligned}
\lambda_1 &= 3X_1^2 + aZ_1^4 = 3(X_1 + Z_1^2)(X_1 - Z_1^2) \\
Z_3 &= 2Y_1Z_1 \\
\lambda_2 &= 4X_1Y_1^2 \\
X_3 &= \lambda_1^2 - 2\lambda_2 \\
\lambda_3 &= 8Y_1^4 \\
Y_3 &= \lambda_1(\lambda_2 - X_3) - \lambda_3
\end{aligned}
$$

http://cs.ucsb.edu/~koc/ac/docs/w03/ecc-protocols.pdf

Elliptic curve point multiplication

- adding a point along an elliptic curve to itself repeatedly
- used in ECC as a means of producing a trapdoor function
- determining n from $Q = nP$ given known values of Q and P
- elliptic curve discrete logarithm problem

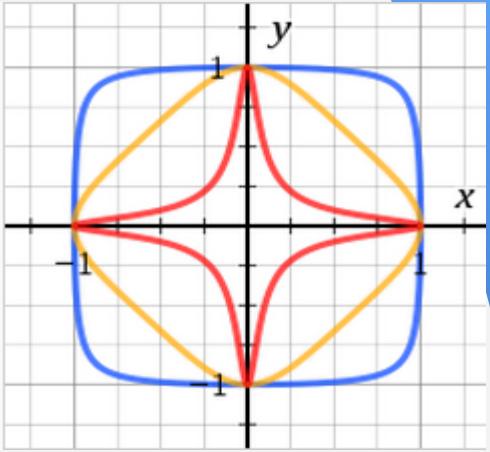
Point multiplication (Double-and-add)

- compute dP with the following representation:

$$d = d_0 + 2d_1 + 2^2 d_2 + \cdots + 2^m d_m$$

```
Q = 0
for i from m to 0 do
  Q := 2Q (using point doubling)
  if di = 1 then Q := Q + P (using point addition)
Return Q
```

Edwards curve



- a new normal form for elliptic curves
- The original form the equation Edwards studied was

$$x^2 + y^2 = c^2(1 + dx^2y^2)$$

solved over a field F whose characteristic is not equal to 2 and c,d are in field F

- Bernstein and Lange gave a slightly simpler form

$$x^2 + y^2 = 1 + dx^2y^2$$

Point Addition

- Addition of two points (x_1,y_1) and (x_2,y_2)

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

- Unified and complete
- 10M + 1S

Inverted Edwards

- Edwards Curve in Inverted Coordinate system:

$$(X^2+Y^2)Z^2 = Z^4 + dX^2Y^2$$

- A projective point $(X_1 : Y_1 : Z_1)$ corresponds to the affine point $(Z_1/X_1, Z_1/Y_1)$ on the Edwards curve
- Unified but not complete
- 9M + 1S

Inverted point addition

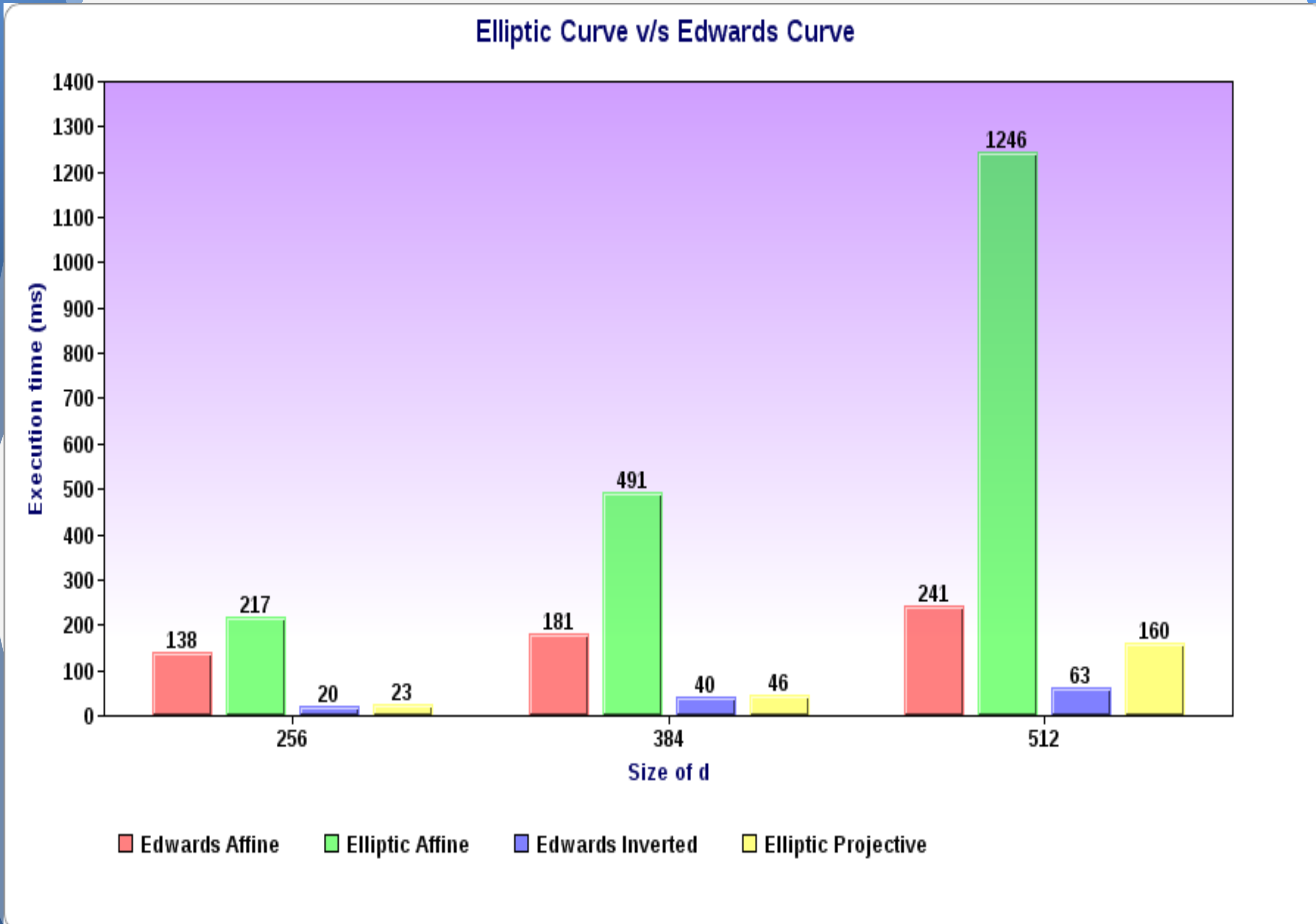
$$(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$$

where

$$X_3 = Z_1 Z_2 (X_1 Y_1 - Y_1 X_2)(X_1 Y_1 Z_2{}^2 2 + Z_1{}^2 X_2 Y_2)$$

$$Y_3 = Z_1 Z_2 (X_1 X_2 + Y_1 Y_2)(X_1 Y_1 Z_2{}^2 - Z_1{}^2 X_2 Y_2)$$

$$Z_3 = k Z_1{}^2 Z_2{}^2 (X_1 X_2 + Y_1 Y_2)(X_1 Y_2 - Y_1 X_2)$$


Elliptic Curve v/s Edwards Curve
Execution time (ms)
1400
1300
1200
1100
1000
900
800
700
600
500
400
300
200
100
0
138
217
20
23
181
491
40
46
241
1246
63
160
256
384
512
Size of d
Edwards Affine
Elliptic Affine
Edwards Inverted
Elliptic Projective

Random Number Generator

- A point (x,y) on the Edwards curve E_d projects to the point (u,v) in the same quadrant on the unit circle as (u,v) = (αx, αy), where

$$\alpha = \frac{1}{\sqrt{x^2 + y^2}}$$

- A point (u,v) on the unit circle projects back to the point (x,y) in the same quadrant on the Edwards curve Ed as (x,y) = (βu, βv),where

$$\beta = \frac{\sqrt{2}}{\sqrt{1 + \sqrt{1 - 4du^2v^2}}}$$

Random Number Generator

A point (x_0,y_0) on the Edwards curve Ed_0 projects to the point (x_1,y_1) in the same quadrant on the Edwards curve Ed_1 as $(x_1,y_1) = (\gamma x_0, \gamma x_1)$, where

$$\gamma = \frac{\sqrt{2}}{\sqrt{x_0^2 + y_0^2 + \sqrt{(x_0^2 + y_0^2)^2 - 4d_1 x_0^2 y_0^2}}}$$

- Random number is obtained by dividing the 'x' coordinate by the value of 'p' which gives a value in the range (0,1)

Conclusion

- Edwards coordinates offer the only complete addition law
- If completeness is not required then Inverted Edwards coordinates are the new speed leader

References

[1] Edwards, Harold. "A normal form for elliptic curves." *Bulletin of the American Mathematical Society* 44.3 (2007): 393-422.

[2] Bernstein, Daniel J., and Tanja Lange. "Faster addition and doubling on elliptic curves." *Advances in cryptology-ASIACRYPT 2007*. Springer Berlin Heidelberg, 2007. 29-50

[3] http://galg.acrypta.com/index.php

[4] http://cs.ucsb.edu/~koc/ac/docs/w03/ecc-protocols.pdf

[5] http://cs.ucsb.edu/~koc/ac/docs/w04/09-ecc.pdf

[6] http://cs.ucsb.edu/~koc/ac/docs/wpp/rng/rng.pdf